



ESTAFAS VÍA SPAM

Recomendaciones para Filtrar: 10 Estafas Enviadas por Correo Electrónico

Si bien hay algunos consumidores que encuentran que los mensajes comerciales masivos no solicitados — conocidos también como correo basura o más comúnmente llamados *spam* — pueden ser informativos, otros creen que son molestos y una gran pérdida de tiempo. Pero también existen otros usuarios de correo electrónico que descubren que el *spam* puede ser costoso: Estos son aquellos que han perdido dinero respondiendo a mensajes de tipo *spam* con ofrecimientos falsos y promociones fraudulentas.

Varios proveedores de servicio de Internet y fabricantes de productos de computación ofrecen filtros para limitar el acceso de mensajes *spam*. Además, hay algunas recomendaciones que pueden ayudarlo a ahorrar tiempo y dinero para evitar la recepción de fraudes por correo electrónico. Alerta en Línea desea que los usuarios de computadoras pasen por el filtro los mensajes *spam* para detectar las estafas, envíen los mensajes *spam* indeseados a las autoridades de seguridad correspondientes y luego, borren los mensajes *spam*. A continuación se describe cómo detectar las 10 estafas más comunes de *spam*:

1. La estafa “Nigeriana” en versión electrónica

La carnada: Mensajes electrónicos enviados por estafadores oportunistas que afirman ser funcionarios, gente de negocios o cónyuges viudos o viudas de líderes gubernamentales de Nigeria o de algún otro país cuyo dinero se encuentra de alguna manera retenido por un período de tiempo limitado. Estos estafadores le ofrecen transferir grandes sumas de dinero a su cuenta bancaria si usted les paga un cargo o “impuestos” para ayudarlos a acceder a su dinero. En caso de que usted responda al ofrecimiento inicial, puede recibir documentos que aparentan ser “oficiales”. Luego, le pedirán que envíe dinero para cubrir los costos de transacción y transferencia y los honorarios del abogado, y también le solicitarán una hoja de papel membreteado en blanco, los números de su cuenta bancaria u otra información. También es posible que hasta lleguen a alentarlos a viajar a Nigeria o un país fronterizo para completar la transacción. Algunos defraudadores han llegado al extremo de llenar cofres con dinero estampado o con papel timbrado para verificar sus declaraciones.

La trampa: Los mensajes electrónicos provienen de delincuentes que están intentando robarle su dinero o perpetrar el robo de identidad. Inevitablemente, surgen algunas emergencias que requieren que usted entregue más dinero demorando la “transferencia” de fondos a su cuenta; al final de la historia, usted no recibe ningún beneficio y el estafador desaparece con su dinero. Según lo que informa el Departamento de Estado, algunas personas que han respondido a solicitudes de “pago por adelantado” de este tipo han sido golpeadas, han resultado víctimas de amenazas y extorsión y en algunos casos, han sido asesinadas.



ESTAFAS VÍA SPAM

Su red de seguridad: Si recibe un mensaje de correo electrónico de parte de alguien que le dice necesitar su ayuda para sacar dinero de un país extranjero, no responda.

Reenvíe las estafas “Nigerianas” — incluyendo toda la información de dirección electrónica — a spam@uce.gov. Si ha perdido dinero con una de estas estafas, llame a la oficina local o más cercana a su domicilio del Servicio Secreto de los Estados Unidos. Encontrará los datos de estas oficinas en las páginas azules de su guía telefónica.

2. Phishing

La carnada: Mensajes electrónicos o de aparición automática (*pop-up messages*) que dicen provenir de un negocio u organización con quien usted posiblemente mantenga una relación comercial — digamos por ejemplo, un proveedor de servicio de Internet (ISP), banco, servicio de pago en línea o hasta una agencia gubernamental. Mediante el texto del mensaje electrónico es posible que se le solicite que “actualice”, “valide” o “confirme” la información de su cuenta, y que en caso de no hacerlo, podría enfrentar graves consecuencias.

La trampa: *Phishing* es el nombre dado en inglés a una estafa mediante la cual los defraudadores envían mensajes de tipo *spam* o *pop-up* para “pescar” información personal y financiera engañando a las víctimas inadvertidas. Los enlaces incluidos en los mensajes lo redirigen a un sitio Web que tiene el mismo aspecto que el de un sitio electrónico de una organización legítima. Pero en realidad es un sitio Web falso cuyo único fin es el de engañarlo para que usted divulgue su información personal para que los operadores puedan robarla, falsear su identidad y gastar a cuatro manos o cometer delitos en su nombre.

Su red de seguridad: Póngase como regla no responder nunca a los mensajes electrónicos o *pop-up* que le soliciten su información personal o financiera ni hacer clic sobre los enlaces incluidos en los mensajes. No utilice la función de cortar y pegar (*cut and paste*) para copiar un enlace en su navegador de Internet, puede ser que los “pescadores de información” o *phishers* logren crear enlaces que aparenten dirigirlo hacia un sitio electrónico cuando en realidad lo llevan a otro sitio parecido. Si está preocupado sobre la seguridad de su cuenta, comuníquese con la organización utilizando un número de teléfono que le conste como genuino o abra una nueva sesión de navegación en el Internet y escriba usted mismo la dirección Web correcta de la compañía. También puede ser de ayuda utilizar un programa antivirus y un *firewall* y mantenerlos actualizados.

Reenvíe los mensajes electrónicos de *phishing* a spam@uce.gov y a la organización cuyo nombre se haya invocado engañosamente.



ESTAFAS VÍA SPAM

3. Estafas de trabajo en casa

La carnada: Mensajes electrónicos que incluyen anuncios que prometen ingresos fijos a cambio de un mínimo esfuerzo — procesamiento de reintegros médicos, rellenado de sobres, tareas de ensamblado de artesanías u otros trabajos. En todos los anuncios se utilizan los mismos tipos de “guiños”: Dinero en efectivo inmediato. Esfuerzo mínimo. Cero riesgo. Y la ventaja de trabajar desde su casa cuando a usted le sea conveniente.

La trampa: Lo que no dicen los anuncios es que es posible que tenga que trabajar muchas horas sin recibir pago ninguno o pagar costos no declarados para colocar anuncios en los periódicos, hacer fotocopias o para comprar materiales, software o equipos para realizar el trabajo. Una vez que usted desembolse su dinero y dedique su tiempo, probablemente se encontrará con promotores que se nieguen a pagarle, pretextando que su trabajo no cumple con sus “estándares de calidad”.

Su red de seguridad: La Comisión Federal de Comercio (FTC) todavía no ha encontrado ninguna persona que se haya hecho rica rellenando sobres o armando imanes para la refrigeradora desde la comodidad de su casa. Los promotores de negocios legítimos de trabajo en casa le deben informar — por escrito — qué es lo que está exactamente comprendido en el programa que venden. Antes de comprometerse a poner su dinero, averigüe cuáles son las tareas que tendrá que realizar, si le pagarán un salario o trabajará a comisión, quién le pagará a usted, cuándo recibirá su primer cheque de pago, el costo total del programa — incluyendo materiales, equipos o cargos por membresía o inscripción — y qué es lo que obtendrá a cambio de su dinero. ¿Puede usted verificar la información de otras personas que estén trabajando actualmente? Tenga cuidado con los “ganchos”, estos son individuos que cobran para mentir y darle todas las razones necesarias para que usted pague para trabajar. Si fuera necesario, procure el consejo profesional de un abogado, contador o asesor financiero o cualquier otro experto y verifique la legitimidad de la compañía consultando a su agencia local de protección del consumidor, oficina del Fiscal General estatal y el *Better Business Bureau* tanto de la localidad en la que se encuentra situada la compañía como también la de su lugar de residencia.

Reenvíe los mensajes electrónicos de estafas de trabajo en casa a spam@uce.gov.

4. Pérdida de peso

La carnada: Mensajes electrónicos que prometen una píldora revolucionaria, un parche, crema u otro producto cuyo resultado será la pérdida de peso sin necesidad de hacer dieta o ejercicio físico. Sobre algunos de los productos promocionados por correo electrónico se afirma que bloquean la



ESTAFAS VÍA SPAM

absorción de la grasa, hidratos de carbono o calorías; sobre otros se garantiza un adelgazamiento permanente; y hasta se llega a afirmar que consumiendo algunos otros productos usted perderá peso a la velocidad de la luz.

La trampa: Estos son trucos ingeniosos que se aprovechan de su optimismo. No existe nada que esté disponible a través del correo electrónico que usted pueda tomar, ponerse en el cuerpo o aplicarse sobre la piel que pueda causar un adelgazamiento permanente ni tampoco considerable.

Su red de seguridad: Los expertos en el tema concuerdan en que la mejor manera de bajar de peso es ingerir menor cantidad de calorías y aumentar el nivel de actividad física para quemar más energía. Un objetivo razonable de adelgazamiento es aproximadamente una libra por semana. Para la mayoría de las personas, esto significa reducir aproximadamente 500 calorías de su dieta diaria, comer una variedad de alimentos nutritivos y hacer ejercicio físico regularmente. La pérdida de peso permanente se produce haciendo cambios permanentes en el estilo de vida. Consulte a su profesional médico para que le recomiende un programa de nutrición y ejercicio físico adaptado a su estilo de vida y metabolismo.

Reenvíe los mensajes electrónicos sobre pérdida de peso a spam@uce.gov.

5. Loterías extranjeras

La carnada: Mensajes electrónicos que ostentan tentadoras chances de ganar en loterías extranjeras. ¡Es posible que hasta reciba un mensaje proclamando que usted ya ha ganado! Solamente tiene que pagar para obtener su premio o cobrar su pozo ganador.

La trampa: La mayoría de las promociones de loterías extranjeras son falsas. Participar de una lotería extranjera es ilegal en los EE.UU. Los estafadores se quedarán con todo el dinero que usted les envíe en concepto de “impuestos” o cargos. Además, los “cazafortunas” que operan estas loterías utilizan los números de la cuenta bancaria de las víctimas para hacer extracciones no autorizadas o los números de sus tarjetas de crédito para hacer cargos adicionales.

Su red de seguridad: Pase por alto estos ofrecimientos. No envíe dinero hoy bajo la promesa de recibir un pago mañana.

Reenvíe los mensajes electrónicos de promociones de loterías extranjeras a spam@uce.gov.

6. Productos cura-todo

La carnada: Mensajes electrónicos que proclaman que un producto es una “cura milagrosa”, una “innovación científica”, un “remedio antiquísimo” — o una cura rápida y efectiva para una amplia variedad de dolencias o enfermedades. Generalmente se anuncian cantidades disponibles limitadas,



ESTAFAS VÍA SPAM

se requiere el pago por adelantado y se ofrecen sin riesgo “con garantía de devolución del dinero”. No es raro que en estos mensajes se incluyan historias clínicas o testimonios de consumidores o médicos declarando resultados asombrosos.

La trampa: No existe ningún producto o suplemento dietario disponible por correo electrónico que pueda cumplir con sus declaraciones sobre la disminución del tamaño de los tumores, cura del insomnio, cura de la impotencia, tratamiento del mal de Alzheimer y prevención de la pérdida aguda de la memoria. Este tipo de declaraciones involucra el tratamiento de enfermedades; las compañías que deseen hacer declaraciones de este tipo deben seguir el procedimiento de prueba y revisión previo a la comercialización que requiere la FDA para todas las medicinas nuevas.

Su red de seguridad: Al momento de evaluar las declaraciones relacionadas al tratamiento de la salud, sea escéptico. Consulte a un profesional médico antes de comprar cualquier producto “cura-todo” del que se diga que puede tratar una amplia variedad de dolencias u ofrezca curas rápidas y soluciones fáciles para enfermedades graves. En términos generales cura-todo se traduce como cura-nada.

Reenvíe los mensajes *spam* que contengan declaraciones sobre curas milagrosas a spam@uce.gov.

7. Estafas de sobrepago de cheques

La carnada: Mensajes electrónicos recibidos en respuesta a un anuncio de venta o subasta en línea colocado por usted, ofreciéndole pagar con un cheque de caja, personal o de una empresa. A último minuto, el individuo que se hace pasar por comprador (o el “agente” del comprador) argumenta alguna razón para emitir el cheque por un monto superior al precio de compra y le pide a usted que le gire la diferencia después de depositar el cheque.

La trampa: Si deposita el cheque, pierde. Generalmente, los cheques son falsificados pero son lo suficientemente buenos para engañar a los cajeros de banco inadvertidos; luego, cuando son rechazados usted es responsable de cubrir el monto total.

Su red de seguridad: No acepte un cheque por un monto superior al de su precio de venta sin importar cuán tentador pueda ser el argumento o lo convincente de la historia que le cuenten. Pídale al comprador que extienda el cheque por el monto del precio de compra. Si el comprador le envía un cheque por un monto incorrecto, devuélvaselo. No envíe la mercadería. Todo vendedor que acepte pagos en cheque, puede solicitar que le entreguen un cheque emitido sobre un banco local o cualquier banco que tenga una sucursal local. De esta manera usted puede apersonarse en el banco para asegurarse de que el cheque sea válido. Si no pudiera ir personalmente, llame al banco sobre el que se emitió el cheque utilizando el número que figura en la guía telefónica, el que obtenga en servicio de informaciones de abonados telefónicos o a través de un sitio de Internet



ESTAFAS VÍA SPAM

conocido y confiable, y no al que le dé el emisor del cheque. Cuando se comunique con el banco, consulte su validez.

Reenvíe los mensajes electrónicos de estafas de sobrepago de cheques a spam@uce.gov y a la oficina de su Fiscal General estatal. Puede averiguar los datos de la oficina de su Fiscal General estatal consultando en el Internet www.naag.org.

8. Ofrecimientos de crédito que requieren un pago adelantado

La carnada: Mensajes electrónicos que le anuncian que ha sido “precalificado” para obtener una tarjeta de crédito o un préstamo con una tasa de interés baja, o que ofrecen reparar sus malos antecedentes de crédito a pesar de que los bancos han rechazado sus solicitudes de crédito o préstamo. Para obtener lo que le ofrecen, usted tiene que adelantar el pago de un cargo de procesamiento de varios cientos de dólares.

La trampa: Un ofrecimiento precalificado legítimo significa que usted ha sido seleccionado *para presentar una solicitud*. Usted aún tiene que completar un formulario de solicitud de crédito o préstamo y todavía se lo pueden denegar. Si usted paga un cargo por adelantado por la promesa de un préstamo o tarjeta de crédito ha sido engañado. Es posible que exista una lista de prestadores, pero ningún préstamo, y la persona a la que usted le pague, se quedará con su dinero y desaparecerá.

Su red de seguridad: No pague a cambio de una promesa. Los prestadores que operan legítimamente nunca “garantizan” una tarjeta o préstamo antes de que usted lo solicite. Las entidades de préstamo legítimas pueden solicitarle que pague un cargo de solicitud, evaluación/ tasación o de informe de crédito, pero es poco frecuente que le requieran el pago de estos cargos antes de que el prestador sea identificado y de que usted complete la solicitud. Además, los cargos generalmente se le pagan directamente al prestador y no al agente o persona que tramitó el préstamo “garantizado”.

Reenvíe los mensajes electrónicos no solicitados que contengan ofrecimientos de crédito a spam@uce.gov.

9. Alivio de deuda

La carnada: Mensajes electrónicos que promocionan una forma de consolidar sus facturas en un pago mensual sin tomar dinero prestado; detener el acoso de acreedores, ejecuciones hipotecarias, incautaciones, gravámenes impositivos y embargos; o bien una manera de borrar sus deudas.



ESTAFAS VÍA SPAM

La trampa: Estos ofrecimientos con frecuencia comprenden procedimientos de bancarrota o quiebra, pero rara vez lo explicitan. Si bien la bancarrota es una forma de lidiar con problemas financieros serios, generalmente se la considera la opción de último recurso. La razón: tiene un impacto negativo de largo plazo sobre su capacidad de obtener crédito y su solvencia financiera. Una declaración de bancarrota figurará en sus informes de crédito por un período de 10 años, y esto puede presentarle dificultades para obtener crédito, empleo, seguro o hasta para conseguir un lugar para vivir. Y encima de todo, probablemente tenga que pagar los honorarios del abogado por la tramitación de los procedimientos de bancarrota.

Su red de seguridad: Cuando vea estos mensajes electrónicos, lea entrelíneas. Antes de recurrir a la quiebra o bancarrota, hable con sus acreedores sobre la posibilidad de llegar a un acuerdo estableciendo un plan de pago modificado, comuníquese con un servicio de asesoría de crédito para que lo ayuden a desarrollar un plan de repago o considere cuidadosamente una segunda hipoteca o línea de crédito con garantía sobre el valor líquido de su vivienda (*home equity line of credit*). Una advertencia: Si bien un préstamo de este tipo puede permitirle consolidar sus deudas, también se le exigirá que ponga su casa como garantía colateral del préstamo. Si no puede cumplir con los pagos, podría perder su casa.

Reenvíe los mensajes *spam* con ofrecimientos de alivio de deuda a spam@uce.gov.

10. Esquemas fraudulentos de inversiones

La carnada: Mensajes electrónicos que promocionan “inversiones” que prometen altas tasas de retorno o ganancia con poco o nada de riesgo. Una de las versiones de esta estafa está a la búsqueda de inversores para formar un banco *offshore*. Otros ofrecimientos de este tipo dan una vaga información sobre la naturaleza de la inversión y enfatizan las tasas de retorno. Los promotores exageran su alto nivel de conexiones financieras; su acceso privilegiado a información confidencial; y prometen que garantizarán la inversión o que se la volverán a comprar. Para cerrar el trato, con frecuencia se basan en estadísticas falsas, tergiversando la importancia de un evento de actualidad o poniendo el acento en la calidad exclusiva de sus ofrecimientos.

La trampa: Muchos de estos esquemas no solicitados son una buena inversión para sus promotores pero no así para los participantes. Los promotores de inversiones fraudulentas operan una estafa en particular por un corto período de tiempo y gastan rápidamente el dinero que obtienen. A menudo, reinician sus operaciones con otro nombre para vender otra estafa de inversiones.



ESTAFAS VÍA SPAM

Su red de seguridad: Tómese su tiempo para evaluar la legitimidad de un ofrecimiento de este tipo: Cuanto más alta es la tasa de rendimiento de su inversión, más alto es el riesgo. No se deje presionar por un promotor para comprometerse en una inversión antes de que esté seguro de su legitimidad. Asimismo, contrate usted mismo a un abogado o contador para que revise el ofrecimiento de inversión.

Reenvíe los mensajes spam que contengan promociones de esquemas fraudulentos de inversiones a spam@uce.gov.

Defiéndase

Los estafadores oportunistas son inteligentes y astutos y están ideando constantemente nuevas variaciones de estafas perpetradas desde tiempos inmemoriales. Pero aún así, los consumidores escépticos pueden detectar las promociones cuestionables y desagradables que se ofrecen por correo electrónico. En caso de que usted reciba un mensaje de correo electrónico que le parezca fraudulento, reenvíelo a la FTC, spam@uce.gov, borre el mensaje y sonría. De esta manera, usted cumplirá con su parte ayudando a sacar del camino a un estafador oportunista.

Alerta en Línea ofrece recomendaciones prácticas brindadas por el gobierno federal y la industria tecnológica para ayudarlo a protegerse contra el fraude en el Internet, mantener su computadora segura y proteger su información personal.

Septiembre 2005